Proceedings of the 19th Conference on Computer Science and Intelligence Systems (FedCSIS) pp. 695–700
DOI: 10.15439/2024F3909
ISSN 2300-5963 ACSIS, Vol. 39

Efficiency and Reliability of Avalanche Consensus Protocol in Vehicular Communication Networks

Saeed Ullah
Quaid I Azam University
Islamabad Pakistan
Email: saeed.ullah@ele.qau.edu.pk

Zaib Ullah
Università Telematica Giustino Fortunato
Benevento Italy
Email: z.ullah@unifortunato.eu

Abdullah Waqas
National University of Technology
Islamabad Pakistan
Email: abdullah@nutech.edu.pk

***Abstract*—In vehicular communication networks, centralized systems face significant security challenges, including privacy preservation, secure authentication, threats from compromised authorities, latency, and throughput. We propose a blockchain-based system that decentralizes control, enhances throughput, and optimizes latency. By leveraging the Avalanche consensus protocol, our solution assures efficient, secure, and robust communication within vehicular networks, mitigating risks associated with centralized control. Our proposed system achieves a substantial throughput, with the Practical Byzantine Fault Tolerance (PBFT) protocol registering 12.8 transactions per second (TPS), and the Avalanche protocol demonstrates an impressive 1007 TPS for 100 validators. Regarding the delay, PBFT experiences 6.61 seconds, whereas Avalanche protocol achieves a remarkably low delay of just one millisecond, both with 100 validators. These findings highlight the superiority of our proposed system in terms of low latency, and enhanced transaction throughput, essential for future vehicular communication systems.**

I. Introduction

IN RECENT years, blockchain technology has emerged as a transformative solution for enhancing security and decentralization across various domains. Originally conceived for cryptocurrencies, blockchain's immutable and distributed ledger system offers robust security features, making it an attractive option for applications requiring secure and transparent data handling. The effective use of blockchain technology plays a crucial role in building smart cities [1]. Additionally, blockchain technology is vital in monitoring systems that assist elderly and impaired patients in adhering to their medication regimens at home. By leveraging blockchain, these systems ensure that all patient-related activities are securely logged and verified, providing a reliable and secure framework for patient care management [2].

In the realm of vehicular communication, where issues such as privacy preservation [3], secure authentication, and protection against insider threats are paramount, blockchain presents a promising approach to address these challenges. By decentralizing control and eliminating single points of failure, blockchain can significantly enhance the resilience and trustworthiness of vehicular communication networks.

Numerous researchers have explored the application of blockchain in vehicular communication to mitigate security vulnerabilities. For instance, studies have proposed the use of blockchain for secure vehicular identity management and authentication, aiming to prevent unauthorized access and ensure that only legitimate vehicles can communicate within the network. Additionally, blockchain-based solutions have been developed to safeguard data integrity and privacy, ensuring that sensitive information shared between vehicles remains confidential and tamper-proof. Despite these advancements, the centralized nature of some proposed solutions still poses risks, as centralized authorities can be single points of failure or targets for attacks [4].

Moreover, the challenge of achieving high transactions per second (TPS) in vehicular communication networks has been a significant hurdle. Traditional blockchain systems, such as Bitcoin and Ethereum, are often criticized for their limited scalability and low TPS, which are insufficient for the high-frequency data exchanges required in vehicular networks. Various consensus mechanisms, including Proof of Work (PoW) and Proof of Stake (PoS), have been explored to improve scalability, but they often fall short of meeting the stringent performance requirements of vehicular communication. To address these issues, we introduce a novel consensus algorithm based on the Avalanche protocol, an innovative and scalable method designed to enhance TPS while maintaining high security standards. Our approach demonstrates the potential to achieve 1007 TPS with 100 validators, providing a robust and efficient framework for secure and high-performance vehicular communication networks.

The rest of the paper is organized as follows: **Section 2** dives into the technical foundation, covering blockchain's secure ledgers and consensus mechanisms. **Section 3** introduces the core functionalities of blockchain technology and provides the groundwork for understanding our proposed solution. **Section 4** defines the system model for secure vehicular communication. **Section 5** provides analyses of the attained results. **Section 6** explores the challenges and promising future research directions. Finally, **Section 7** concludes the article by summarizing the key findings.

II. Technical Background

Blockchain technology is a distributed ledger system that securely, transparently, and immutably records transactions. Each block in the chain contains a list of transactions, a timestamp, and a cryptographic hash of the preceding block, creating an alteration-resistant record. This decentralized architecture eliminates single points of control, fostering security and trust among participants [5].

In a blockchain network, participants initiate and broadcast transactions across the network. Validators, also known as miners in some systems, collect these transactions into blocks. Before adding a block to the blockchain, a consensus mechanism ensures its validity by achieving network-wide agreement on the included transactions. This process prevents double-spending and safeguards against fraudulent activities [5].

The consensus mechanism is a fundamental component of blockchain technology, as it guarantees the integrity and consistency of the distributed ledger. A variety of consensus mechanisms exist, each with its strengths and weaknesses. Proof of Work (PoW) [6], used by Bitcoin blockchain, requires validators to solve complex cryptographic puzzles, which ensures security but is energy-intensive and slow [5], [7]. Proof of Stake (PoS) [6], on the other hand, selects validators based on their stake in the network, which is more energy-efficient but can lead to centralization if a few participants hold large stakes [8]. The consensus mechanism validates transactions determines how the blockchain grows and ensures that all copies of the distributed ledger are synchronized across the network [9], [10], [11].

In vehicular communication, where rapid data exchange and high security are paramount, traditional consensus mechanisms often prove inadequate. The high latency and low throughput associated with PoW and PoS make them unsuitable for the real-time demands of vehicular networks. These limitations have prompted researchers to explore alternative consensus algorithms that can provide higher TPS while maintaining robust security standards. One such innovative approach is the Avalanche consensus protocol, which uses repeated sampling and confidence levels to achieve rapid consensus without the need for extensive computational resources. By leveraging the Avalanche protocol, it is possible to significantly improve the TPS in vehicular communication networks, addressing one of the major bottlenecks in existing blockchain solutions.

For instance, studies have proposed blockchain-based identity management systems for vehicles. These systems leverage the blockchain's immutable ledger to store and verify vehicle identities, enhancing trust and preventing unauthorized access within the network [12], [13], [14], [15], [16], [17]. Additionally, blockchain's ability to provide a tamper-proof record of transactions makes it well-suited for preserving the privacy and integrity of data exchanged between vehicles [18], [19], [20]. However, these solutions still face challenges related to scalability and performance, highlighting the need for more efficient consensus mechanisms like the Avalanche protocol discussed earlier.

Integrating blockchain with machine learning in vehicular communication networks can significantly enhance security, efficiency, and data analysis capabilities. Blockchain can provide a secure and immutable data storage solution, ensuring the integrity and privacy of the data collected from vehicles. Machine learning algorithms can then analyze this data to predict traffic patterns, optimize routing, and enhance autonomous driving capabilities. For instance, secure data sharing through blockchain can support federated learning models, where decentralized data can be collaboratively processed without compromising privacy [21], [22]. This integration creates a robust framework for real-time decision-making and continuous improvement of vehicular systems.

The Avalanche consensus protocol [23] represents a promising advancement in this field. By enabling high TPS and reducing latency, it addresses the critical performance issues that have hindered the adoption of blockchain in vehicular communication. The proposed system, which achieves 1007 TPS with 100 validators, demonstrates the potential of Avalanche to meet the strict requirements of vehicular networks, providing a secure, decentralized, and high-performance solution for future applications.

III. Introduction to Blockchain and Consensus Mechanisms

In the following, we briefly explore the fundamentals of blockchain technology and consensus mechanisms.

A. Blockchain

Blockchain technology, originally conceived as the foundation for Bitcoin cryptocurrency, has rapidly transformed into a versatile solution across diverse industries, including vehicular communication networks. At its core, it functions like a public record book, not controlled by a single entity but maintained by a distributed network of computers. This distributed ledger, called a blockchain, consists of interconnected blocks as shown in Fig. 1 [24], each containing a list of transactions. These transactions can represent anything of value, such as financial transfers or ownership records.

The core strength of blockchain lies in its decentralization, eliminating the need for a central authority and making it resistant to manipulation. Additionally, the immutability of transactions, meaning they cannot be altered once recorded, ensures data integrity and transparency. Cryptographic techniques further secure the blockchain, offering a robust shield against tampering and fraud.

In the context of vehicular communication, blockchain offers significant advantages. It can facilitate secure and reliable data exchange among vehicles and infrastructure, addressing critical concerns like unauthorized access and data manipulation. The tamper-proof nature of blockchain also helps preserve the privacy of data exchanged between vehicles. Furthermore, the decentralized architecture enhances the resilience of vehicular communication networks by eliminating single points of failure. However, existing solutions leveraging blockchain in this domain still face challenges related to

Fig. 1. Blockchain Technology

scalability and performance. This is where innovative consensus mechanisms like the Avalanche protocol come into play, aiming to address these limitations by achieving high transaction throughput and low latency, paving the way for secure and efficient vehicular communication networks of the future.

B. Consensus Algorithm

The consensus algorithm is a critical component of blockchain technology, ensuring that all distributed nodes agree on the state of the ledger. The primary goal is to enable each node to verify block generation in a decentralized manner, typically by selecting one validator or miner per round to add a new block. Three common consensus algorithms are Proof of Work (PoW), Proof of Stake (PoS), and PBFT. In PoW, validators compete by solving complex cryptographic puzzles, while PoS relies on validators who have staked cryptocurrency to participate in block creation.

1) Practical Byzantine Fault Tolerance: The PBFT consensus algorithm employs a two-thirds majority voting method, making it suitable for private blockchains where trusted participants are known. It's commonly used in systems like IBM Hyperledger Fabric. As illustrated in Fig 2, the PBFT process involves distinct stages: REQUEST, PRE-PREPARE, PREPARE, COMMIT, and REPLY [25]. To understand how Byzantine faults are tolerated, here's a breakdown of the PBFT process:

1) **Request:**
   - The client initiates the process by broadcasting a transaction to all nodes in the network.
2) **Pre-Prepare:**
   - The primary node, selected through a pre-defined process or upon receiving the first client message, assembles a block containing the received transaction(s).
   - This block is then broadcast to all replica nodes in the network.
3) **Prepare:**
   - Upon receiving the pre-prepared block, each replica node verifies two things:
     a) Whether it has received the same pre-prepared block from the primary node.
     b) Whether the transactions and values within the block are valid according to the system's rules.
   - If both conditions are met, the replica node broadcasts a "prepare" message for the block.
4) **Commit:**
   - Once a replica node receives "prepare" messages from more than two-thirds of the other nodes (including the primary node), it can be confident that the block is legitimate.
   - This threshold ensures resistance to Byzantine faults, where nodes might malfunction or provide malicious information.
   - At this stage, the replica node broadcasts a "commit" message for the block.
5) **Reply:**
   - Finally, all nodes, including the primary and replica nodes, send a reply message to the client, indicating successful transaction processing or any potential errors encountered.

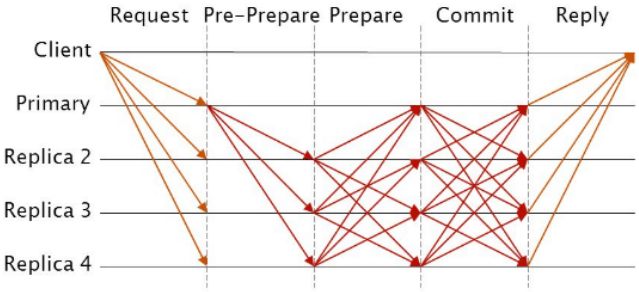

Fig. 2. PBFT Consensus Protocol

2) Avalanche Consensus Protocol: The Avalanche consensus protocol is a unique consensus mechanism designed to achieve high throughput, low latency, and robust security. Here is an overview of the Avalanche consensus algorithm:

1) **Initialization:**
   - Nodes in the network are initialized and are aware of each other. Each node starts with an initial set of transactions it considers valid.
2) **Transaction Propagation:**
   - A node receives a transaction and propagates it to a small, randomly selected subset of nodes (neighbors).
3) **Voting Process**:
   - Each node in the subset checks the validity of the transaction and votes to accept or reject it based on its local view.
   - The voting process involves repeated rounds where nodes query their peers to reach a consensus.
4) **Sampling and Subsampling:**
   - In each round, nodes sample a random subset of other nodes (k nodes) and adopt the decision of the majority within this subset.
   - This process continues until a majority consensus is reached consistently over several rounds.
5) **Confidence Levels:**

- Each node maintains a confidence level for each transaction based on the number of times the transaction is voted as valid in consecutive rounds.
- A transaction is considered finalized when the confidence level surpasses a predefined threshold.

6) **Finalization:**

- Once the confidence threshold is reached, the transaction is finalized and accepted by the network.

IV. System Model

The proposed system model for secure and efficient vehicular communication leverages the Avalanche consensus protocol to address the inherent challenges of achieving high throughput and low latency in vehicular networks. This system model includes several key components and mechanisms designed to ensure robust security, privacy, and performance.

The vehicular network, depicted in Figure 3 as a dynamic Vehicular Ad Hoc Network (VANET) [26], comprises a large number of vehicles acting as nodes in a decentralized blockchain network. Each vehicle is equipped with a communication module capable of interacting with other vehicles and the blockchain network. These vehicles perform dual roles: they act as both users initiating transactions and validators participating in the consensus process.

To initiate a transaction, a vehicle broadcasts its message to the network. This message may include data such as vehicle identity, location, or other relevant information necessary for the intended application (e.g., traffic management, collision avoidance). The transaction is then received by neighboring vehicles, which subsequently propagate the transaction across the network.

Each transaction is grouped into a block by a validator. Unlike traditional PoW and PoS systems, the proposed model employs the Avalanche consensus protocol, which is well-suited for environments requiring rapid consensus and high transaction throughput. Validators in the Avalanche protocol operate by continuously sampling the network to determine the confidence level of each transaction. This process involves selecting a small, random subset of validators and querying their opinions on the validity of a transaction. Validators update their own state based on the responses received, and this process is repeated multiple times until a predefined confidence threshold is met.

The confidence level is a critical parameter in this model. It determines the number of repeated sampling rounds necessary to reach consensus. This parameter is set to ensure a balance between security and performance, allowing the system to maintain high throughput while providing strong guarantees against attacks and inconsistencies.

To enhance security and privacy, the system model includes mechanisms for secure authentication and identity management. Each vehicle is issued a unique cryptographic key pair, which it uses to sign its transactions. This ensures that only authorized vehicles can participate in the network and provides a means for verifying the integrity and authenticity of each transaction. Additionally, the blockchain's immutable ledger

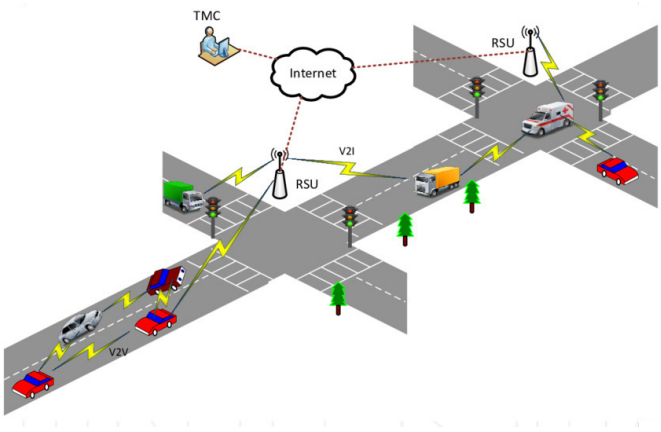

Fig. 3. Vehicular Ad-hoc Network

serves as a tamper-proof record of all transactions, further enhancing security by making it difficult for malicious actors to alter or forge data.

Privacy preservation is addressed through the use of pseudonymous identities. Vehicles do not reveal their true identities when broadcasting transactions; instead, they use temporary pseudonyms that can be periodically changed to prevent tracking and linking of activities. This approach ensures that while the network maintains a transparent and verifiable record of transactions, the privacy of individual vehicles is preserved.

The proposed system model also includes provisions for handling compromised nodes and insider threats. The Avalanche consensus protocol's reliance on repeated sampling and confidence levels makes it resilient to Sybil attacks and other forms of manipulation. Even if a subset of validators is compromised, the probability of them consistently influencing the consensus process is minimized, ensuring the integrity and reliability of the network.

V. Results

In Figure 4, the comparison of TPS between PBFT and Avalanche consensus mechanisms is illustrated. PBFT achieves a TPS of 12.8 [25], while Avalanche reaches 1007 TPS. This obvious contrast highlights Avalanche's superior scalability and efficiency in processing high volumes of transactions. The increased TPS in Avalanche can be attributed to its probabilistic consensus mechanism, which reduces communication overhead, enabling faster transaction processing compared to the deterministic approach of PBFT.

Figure 5 focuses on the delay experienced in reaching consensus. For a network with 100 validators, PBFT exhibits a delay of 6.61 seconds [25], whereas Avalanche demonstrates a remarkably low delay of just 1 millisecond. This minimal delay in Avalanche is due to its innovative consensus algorithm, which leverages repeated random sampling and metastability to achieve quick and efficient consensus. In contrast, PBFT's higher delay results from its multiple rounds of communication

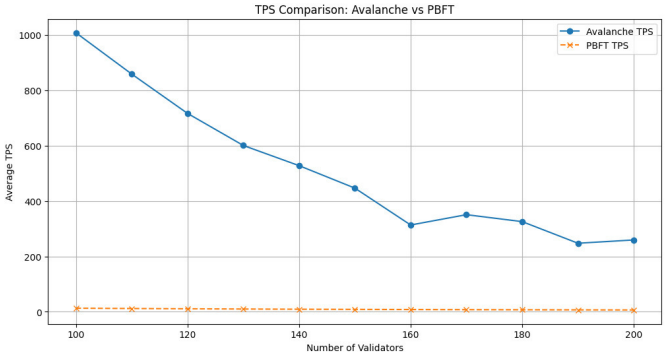

Fig. 4. TPS vs Number of Vlaidators

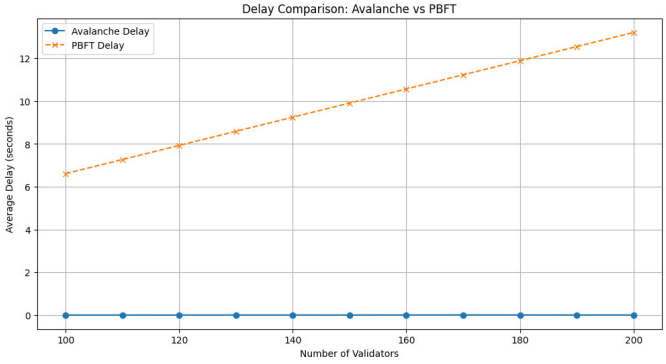

Fig. 5. Delay vs Number of Vlaidators

and voting among validators, which are necessary to ensure fault tolerance.

The implications of these results are particularly significant for vehicle-to-vehicle (V2V) communication systems. High throughput and low latency are critical for the rapid exchange of information necessary for safety and coordination among vehicles. Avalanche's ability to handle a high number of transactions per second with minimal delay makes it a suitable candidate for such applications, ensuring that communication between vehicles is fast, reliable, and efficient. On the other hand, PBFT, with its higher delay and lower TPS, may struggle to meet the stringent requirements of V2V communication, where timely data exchange is paramount.

VI. Challenges and Future Research Directions

The Avalanche protocol offers a glimpse into a future of secure and scalable V2X communication. However, several challenges need to be addressed before widespread adoption:

- Achieving the theoretical throughput of Avalanche in real-world V2X networks with high vehicle density remains an open question.
- Ensuring user privacy through privacy-preserving consensus and data anonymization techniques is essential [27].
- Seamless integration with existing V2X infrastructure requires careful consideration to minimize disruption and ensure compatibility.

Looking towards the future, several research directions hold promise for more efficient and adaptable solutions:

- Hybrid consensus models offer potential for V2X communication but require further research for optimal integration within the V2X ecosystem [28].
- Developing lightweight blockchain clients specifically designed for resource-constrained vehicles can significantly reduce computational overhead and improve energy efficiency.
- Rigorous formal verification of the Avalanche protocol's security properties is essential for wider adoption.
- Developing standard protocols for integrating Avalanche with V2V and V2X communication systems is also essential for wider adoption.

By handling these challenges and pursuing these promising research directions, the Avalanche protocol has the potential to revolutionize V2X communication, paving the way for a secure, reliable, and efficient future for intelligent transportation systems.

VII. Conclusion

Blockchain technology is a cornerstone of decentralized applications, particularly in V2X communication where decentralization is paramount for security and reliability. The Avalanche protocol stands out for its high throughput and low latency, making it a strong candidate for V2X communication. This analysis revealed Avalanche's impressive performance, achieving a TPS of 1007 with a delay of just 1 millisecond for 100 validators, significantly exceeding PBFT's capabilities (TPS: 12.8, delay: 6.61 seconds). These findings highlight Avalanche's potential to effectively address the demanding requirements of modern decentralized applications compared to PBFT. However, unlocking the full potential of Avalanche in V2X networks requires further exploration. Key challenges include achieving scalability in dense real-world scenarios, designing robust incentive mechanisms for validators, and ensuring user privacy through data anonymization techniques. By addressing these challenges and pursuing these advancements, Avalanche has the potential to revolutionize V2X communication, paving the way for a secure, reliable, and efficient future for intelligent transportation systems.

Acknowledgment

This research has been partially funded by the Regione Campania with the "PSR Campania 2014-2022 programme, Misura 16, Tipologia d'intervento 16.1.2." Project: "EVOOLIO - L'Evoluzione dell'Olio EVO Sannita tracciato con la Blockchain.

References

[1] Z. Ullah, M. Naeem, A. Coronato, P. Ribino, and G. De Pietro, "Blockchain applications in sustainable smart cities," *Sustainable Cities and Society*, p. 104697, 2023.

[2] G. Paragliola, A. Coronato, M. Naeem, and G. De Pietro, "A reinforcement learning-based approach for the risk management of e-health environments: A case study," in *2018 14th international conference on signal-image technology & internet-based systems (SITIS)*. IEEE, 2018, pp. 711–716.

[3] A. Coronato, G. de Pietro, and G. Paragliola, "A monitoring system enhanced by means of situation-awareness for cognitive impaired people," in *BodyNets '13: Proceedings of the 8th International Conference on Body Area Networks*. Brussels, BEL: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Sep. 2013, pp. 124–127.

[4] M. Jamal, Z. Ullah, M. Naeem, M. Abbas, and A. Coronato, "A hybrid multi-agent reinforcement learning approach for spectrum sharing in vehicular networks," *Future Internet*, vol. 16, no. 5, p. 152, 2024.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[6] S. Yan, "Analysis on blockchain consensus mechanism based on proof of work and proof of stake," in *2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI)*, 2022, pp. 464–467.

[7] S. S. Mahdi, Z. Ullah, G. Battineni, M. G. Babar, and U. Daood, "The telehealth chain: a framework for secure and transparent telemedicine transactions on the blockchain," *Irish Journal of Medical Science (1971-)*, pp. 1–9, 2024.

[8] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[9] M. Naeem, S. Bashir, M. U. Khan, and A. A. Syed, "Performance comparison of scheduling algorithms for mu-mimo systems," in *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2016, pp. 601–606.

[10] S. Islam, M. J. Islam, M. Hossain, S. Noor, K.-S. Kwak, and S. M. R. Islam, "A survey on consensus algorithms in blockchain-based applications: Architecture, taxonomy, and operational issues," *IEEE Access*, vol. 11, pp. 39 066–39 082, 2023.

[11] M. Jamal, Z. Ullah, and M. Abbas, "Self-adapted resource allocation in v2x communication," in *Workshop Proceedings of the 19th International Conference on Intelligent Environments (IE2023)*, vol. 32. IOS Press, 2023, p. 104.

[12] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for vanets," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2792–2801, 2019.

[13] M. Naeem, G. Paragiola, A. Coronato, and G. De Pietro, "A cnn based monitoring system to minimize medication errors during treatment process at home," in *Proceedings of the 3rd International Conference on Applications of Intelligent Systems*, 2020, pp. 1–5.

[14] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-tsca: Blockchain assisted trustworthiness scalable computation for v2i authentication in vanets," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1386–1396, 2021.

[15] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020.

[16] Q. Feng, D. He, S. Zeadally, and K. Liang, "Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146–4155, 2020.

[17] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, "Bcppa: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 12, pp. 7408–7420, 2021.

[18] A. Alharthi, Q. Ni, and R. Jiang, "A privacy-preservation framework based on biometrics blockchain (bbc) to prevent attacks in vanet," *IEEE Access*, vol. 9, pp. 87 299–87 309, 2021.

[19] G. Paragliola and M. Naeem, "Risk management for nuclear medical department using reinforcement learning algorithms," *Journal of Reliable Intelligent Environments*, vol. 5, pp. 105–113, 2019.

[20] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in vanets," *IEEE Access*, vol. 7, pp. 117 716–117 726, 2019.

[21] A. R. Javed, M. M. Hassan, F. Shahzad, W. Ahmed, S. Singh, T. Baker, and T. R. Gadekallu, "Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey," *Sensors*, vol. 22, no. 12, p. 4394, Jun 2022.

[22] M. Dibaei, X. Zheng, Y. Xia, and X. Xu, "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. PP, no. 99, pp. 1–18, August 2021.

[23] T. Rocket, M. Yin, K. Sekniqi, R. van Renesse, and E. G. Sirer, "Avalanche: A novel metastable consensus protocol family for cryptocurrencies," https://www.avalabs.org/whitepapers, 2020, accessed: 2024-07-06.

[24] G. Bigini, V. Freschi, and E. Lattanzi, "Blockchain in the iot: Architectures and implementation," *Future Internet*, vol. 12, no. 12, p. 208, 2020, submission received: 3 November 2020 / Revised: 20 November 2020 / Accepted: 23 November 2020 / Published: 25 November 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/12/208

[25] J. Noh, S. Jeon, and S. Cho, "Distributed blockchain-based message authentication scheme for connected vehicles," *Electronics*, vol. 9, no. 1, p. 74, 2020.

[26] U. Hernandez-Jayo, A. S. K. Mammu, and I. De-la Iglesia, "Reliable communication in cooperative ad hoc networks," *Contemporary Issues in Wireless Communications*, 2014.

[27] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, vol. 25, p. 100247, 2020.

[28] J. Meijers, P. Michalopoulos, S. Motepalli, G. Zhang, S. Zhang, A. Veneris, and H.-A. Jacobsen, "Blockchain for v2x: Applications and architectures," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 193–209, 2022.